LISTING OF CLAIMS

This listing of claims will replace all prior versions, and listings, of claims of the application:

Claim 1-15 (Canceled)

Claim 16 (New) A method for mutual authentication of a terminal and a network comprising the steps of:

receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2);

sending the first random number (challenge 1) to the terminal;

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2);

authenticating the terminal by matching the first calculated response with the first response (response 1);

sending the second response (response 2) to the terminal; and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with

the second response (response 2).

Claim 17 (New) The method of claim 16, wherein the terminal calculates the first calculated response from the first random number (challenge 1) using an internally stored key.

Claim 18 (New) The method of claim 16, wherein the terminal calculates the second calculated response from the first random number (challenge 1) or from the first calculated response using an internally stored key.

Claim 19 (New) The method of claim 16, wherein multiple triplet data sets are received from the authentication center and stored on the network as a stockpile to reduce the number of times triplet data sets must be received.

Claim 20 (New) The method as claimed in claim 16, wherein to use the first calculated response of the terminal as the second challenge (Challenge 2), a shorter length of the first calculated response is filled out to make up a greater length of the second challenge (Challenge 2).

Claim 21 (New) The method as claimed in claim 20, wherein the filling-out is performed on a subscriber-specific basis;

and

the complete length of the first calculated response is shortened before transmission.

Claim 22 (New) The method as claimed in claim 20, wherein the first calculated response is filled out with defined bits from an internally stored key to make up the length of the second challenge (Challenge 2).

Claim 23 (New) The method as claimed in claim 20, wherein the second challenge (Challenge 2) corresponds to the first calculated response before it was shortened.

Claim 24 (New) The method as claimed in claim 16, wherein the network is a GSM network.

Claim 25 (New) The method as claimed in claim 16, wherein the network is a wire-based network.

Claim 26 (New) The method as claimed in claim 25, wherein components in the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 27 (New) The method as claimed in claim 16, wherein

the authentication center calculates the triplet data sets requested by the network and transmits the calculated triplet data sets to the network off-line and independently of time, on request by the network, and before data interchange between the network and the terminal.

Claim 28 (New) A method for mutual authentication of a terminal and a network comprising the steps of:

receiving, at the network, a triplet data set from an authentication center, the triplet data set including a first random number (challenge 1), a first response (response 1) and a second response (response 2);

sending the first random number (challenge 1) and the second response (response 2) to the terminal as a single data set;

receiving, from the terminal, a first calculated response, calculated by the terminal based on the first random number (challenge 1), wherein the first calculated response is used as a second challenge (challenge 2);

authenticating the terminal by matching the first calculated response with the first response (response 1); and

wherein the network is authenticated by the terminal by matching a second calculated response, calculated by the terminal based on the first random number (challenge 1) with the second response (response 2).

Claim 29 (New) The method of claim 28, wherein the terminal calculates the first calculated response from the first random number (challenge 1) using an internally stored key.

Claim 30 (New) The method of claim 28, wherein the terminal calculates the second calculated response from the first random number (challenge 1) or from the first calculated response using an internally stored key.

Claim 31 (New) The method of claim 28, wherein multiple triplet data sets are received from the authentication center and stored on the network as a stockpile to reduce the number of times triplet data sets must be received.

Claim 32 (New) The method as claimed in claim 28, wherein to use the first calculated response of the terminal as the second challenge (Challenge 2), a shorter length of the first calculated response is filled out to make up a greater length of the second challenge (Challenge 2).

Claim 33 (New) The method as claimed in claim 32, wherein the filling-out is performed on a subscriber-specific basis; and

the complete length of the first calculated response is shortened before transmission.

Claim 34 (New) The method as claimed in claim 32, wherein the first calculated response is filled out with defined bits from an internally stored key to make up the length of the second challenge (Challenge 2).

Claim 35 (New) The method as claimed in claim 32, wherein the second challenge (Challenge 2) corresponds to the first calculated response before it was shortened.

Claim 36 (New) The method as claimed in claim 28, wherein the network is a GSM network.

Claim 37 (New) The method as claimed in claim 28, wherein the network is a wire-based network.

Claim 38 (New) The method as claimed in claim 37, wherein components in the wire-based network are different monitoring units of computers which authenticate themselves with a central computer, and vice versa.

Claim 39 (New) The method as claimed in claim 28, wherein the authentication center calculates the triplet data sets

requested by the network and transmits the calculated triplet data sets to the network off-line and independently of time, on request by the network, and before data interchange between the network and the terminal.